ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINHTRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN **KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

🙟 🙨 🙝



**BÁO CÁO ĐỒ ÁN  
MÔN: LẬP TRÌNH MẠNG CĂN BẢN  
  
Đề tài: Xây dựng ứng dụng quét mạng**

|  |  |  |  |
| --- | --- | --- | --- |
| Giảng viên hướng dẫn | : | ĐẶNG LÊ BẢO CHƯƠNG | |
| Lớp | : | NT106.P12 | |
|  | | | | | | |
| Nhóm thực hiện – Nhóm 23 | | | | |
| 1. Nguyễn Thiện Chí | | | | MSSV: 23520178 |
| 2. Đoàn Thanh Đệ | | | | MSSV: 23520282 |
| 3. Huỳnh Lâm Tuấn Phong | | | | MSSV: 23521162 |

MỤC LỤC

[A. LỜI MỞ ĐẦU 1](#_Toc184888496)

[1. BỐI CẢNH CHỌN ĐỀ TÀI 1](#_Toc184888497)

[1.1. Tổng quan 1](#_Toc184888498)

[1.2. Tầm quan trọng của việc giám sát mạng 1](#_Toc184888499)

[1.3. Mục tiêu đồ án 1](#_Toc184888500)

[2. BẢNG PHÂN CHIA CÔNG VIỆC 2](#_Toc184888501)

[B. NỘI DUNG CHÍNH 3](#_Toc184888502)

[1. TỔNG QUAN CHƯƠNG TRÌNH 3](#_Toc184888503)

[1.1. Một số khái niệm 3](#_Toc184888504)

[1.1.1. Quét mạng 3](#_Toc184888505)

[1.1.2. Bắt gói tin 3](#_Toc184888506)

[1.2. Tính năng xây dựng được 4](#_Toc184888507)

[1.2.1. Tìm các thiết bị trong cùng mạng 4](#_Toc184888508)

[1.2.2. Quét cổng TCP/UDP của một địa chỉ IP 4](#_Toc184888509)

[1.2.3. Lắng nghe thông điệp từ một địa chỉ IP đến giao diện mạng 4](#_Toc184888510)

[1.2.4. Bắt và hiển thị thông tin trên một giao diện mạng 4](#_Toc184888511)

[1.3. Thiết kế chương trình 5](#_Toc184888512)

[1.3.1. Mô hình phân rã chức năng 5](#_Toc184888513)

[1.3.2. Sequence Diagram 6](#_Toc184888514)

[Giải thích từng phần: 6](#_Toc184888515)

[1.3.3. Cơ chế hoạt động của chương trình 7](#_Toc184888516)

[2. PHÂN TÍCH CÁC CODE QUAN TRỌNG 8](#_Toc184888517)

[2.1. Khám phá các thiết bị có trong mạng cục bộ 8](#_Toc184888518)

[2.2. Quét cổng 13](#_Toc184888519)

[2.3. Lắng nghe thông điệp từ địa chỉ đối tượng (Listen Message) 15](#_Toc184888520)

[2.4. Bắt gói tin 16](#_Toc184888521)

[C. Một số thay đổi 20](#_Toc184888522)

[D. VIDEO DEMO 21](#_Toc184888523)

[TÀI LIỆU THAM KHẢO 22](#_Toc184888524)

A. LỜI MỞ ĐẦU

## 1. BỐI CẢNH CHỌN ĐỀ TÀI

### 1.1. Tổng quan

Trong thời đại công nghệ thông tin phát triển mạnh mẽ, bảo mật mạng và phân tích dữ liệu đóng vai trò quan trọng đối với an toàn thông tin và hiệu suất của các hệ thống mạng. Ứng dụng quét mạng và bắt gói tin là công cụ thiết yếu để giám sát, phân tích và phát hiện các mối đe dọa tiềm ẩn trong luồng dữ liệu mạng. Đề tài này được lựa chọn nhằm giúp hiểu rõ hơn về cách thức hoạt động của các ứng dụng này, đồng thời cung cấp kiến thức thực tiễn cho việc quản lý và bảo vệ hệ thống mạng trước các rủi ro bảo mật.

### 1.2. Tầm quan trọng của việc giám sát mạng

* **Đảm bảo tính sẵn sàng và hiệu suất mạng**: Giám sát mạng giúp nhận diện kịp thời các vấn đề như tắc nghẽn, lỗi kết nối hoặc các dịch vụ bị gián đoạn. Điều này cho phép các quản trị viên nhanh chóng xử lý và duy trì hiệu suất hoạt động liên tục của hệ thống.
* **Phát hiện và ngăn chặn mối đe dọa bảo mật**: Quá trình giám sát có thể giúp phát hiện sớm các dấu hiệu xâm nhập bất hợp pháp, các cuộc tấn công mạng như DDoS, hoặc hành vi đáng ngờ trong luồng dữ liệu. Điều này giúp ngăn chặn và bảo vệ hệ thống trước khi các vấn đề trở nên nghiêm trọng.
* **Tối ưu hóa tài nguyên mạng:** Giám sát cho phép các quản trị viên hiểu rõ cách tài nguyên mạng được sử dụng và điều chỉnh để tối ưu hóa hiệu suất. Điều này giúp giảm thiểu chi phí và tăng hiệu quả sử dụng các tài nguyên sẵn có.
* **Hỗ trợ xử lý sự cố nhanh chóng**: Khi xảy ra sự cố, thông tin từ giám sát mạng cung cấp dữ liệu chi tiết giúp xác định nguyên nhân gốc rễ và triển khai giải pháp nhanh chóng. Điều này giảm thiểu thời gian chết và hạn chế tác động tiêu cực đến doanh nghiệp

### 1.3. Mục tiêu đồ án

Áp dụng những kiến thức lập trình có sẵn từ các môn học trước, hướng đến mục tiêu có thể nghiên cứu lâu dài mà vẫn phù hợp với ngành học và chuẩn đầu ra của môn Lập trình mạng căn bản, vì thế nhóm quyết định chọn đề tài ***“Xây dựng ứng dụng quét mạng đơn giản”*** để thực hiện cho đồ án của môn học này.

Việc xây dựng ứng dụng được lấy cảm hứng từ các công cụ quét mạng và bắt gói tin phổ biến hiện nay (ví dụ như Nmap, Wireshark,…). Ứng dụng được thực hiện nhằm đáp ứng các nhu cầu thiết yếu về bảo mật và quản lý mạng một cách đơn giản. Ứng dụng này không chỉ giúp giám sát và phân tích lưu lượng mạng một cách chi tiết mà còn cung cấp các công cụ cần thiết để bắt gói tin, phân tích và xử lý chúng.

## 2. BẢNG PHÂN CHIA CÔNG VIỆC

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Tên | MSSV | Công việc |
| 1 | Nguyễn Thiện Chí | 23520178 | Viết báo cáo (vẽ các diagram), code một số tính năng bonus, tổng hợp đồ án. |
| 2 | Đoàn Thanh Đệ | 23520282 | Code các tính năng chính, thuyết trình. |
| 3 | Huỳnh Lâm Tuấn Phong | 23521162 | Thuyết trình, làm powerpoint. |

B. NỘI DUNG CHÍNH

## 1. TỔNG QUAN CHƯƠNG TRÌNH

### 1.1. Một số khái niệm

#### 1.1.1. Quét mạng

**Quét mạng** là quá trình kiểm tra và phân tích một mạng máy tính để phát hiện các thiết bị kết nối, kiểm tra tình trạng hoạt động của chúng và xác định các lỗ hổng bảo mật tiềm tàng. Việc này có thể bao gồm quét các địa chỉ IP, cổng, và dịch vụ đang chạy trên các thiết bị trong mạng. Các tác dụng của việc quét mạng:

* + Giúp phát hiện các thiết bị không xác định hoặc không được phép kết nối vào mạng.
  + Phát hiện các lỗ hổng bảo mật tiềm tàng như cổng mở không cần thiết hoặc dịch vụ yếu kém.
  + Cung cấp thông tin để tối ưu hóa và quản lý tài nguyên mạng hiệu quả hơn.
  + Cho phép theo dõi trạng thái hoạt động và hiệu suất của các thiết bị kết nối.

**Công cụ thực hiện**: Nmap, Angry IP Scanner, Advanced IP Scanner,…

#### 1.1.2. Bắt gói tin

**Bắt gói tin** (packet capturing) là quá trình thu thập các gói tin dữ liệu truyền qua mạng để phân tích nội dung và hành vi của chúng. Quá trình này giúp xác định các sự cố mạng, phát hiện các cuộc tấn công, và giám sát hoạt động mạng.

* + Cung cấp cái nhìn chi tiết về lưu lượng mạng, bao gồm nội dung các gói tin, địa chỉ nguồn và đích, và các thông tin tiêu đề.
  + Giúp phát hiện và phân tích các sự cố mạng như tắc nghẽn, mất gói, và các cuộc tấn công.
  + Theo dõi và phát hiện các hành vi bất thường hoặc xâm nhập trái phép.

**Công cụ thực hiện**: Wireshark, tcpdump, Microsoft Network Monitor,…

### 1.2. Tính năng xây dựng được

#### 1.2.1. Tìm các thiết bị trong cùng mạng

* Quản lý thiết bị: Giúp quản trị mạng có cái nhìn tổng quan về tất cả các thiết bị đang kết nối vào mạng, bao gồm máy tính, điện thoại, máy in, và các thiết bị IoT.
* Phát hiện thiết bị lạ: Có thể phát hiện các thiết bị không được phép truy cập vào mạng, từ đó ngăn chặn các hành vi xâm nhập trái phép.
* Kiểm tra kết nối: Đảm bảo rằng các thiết bị quan trọng như server, router, và switch đang hoạt động bình thường và có kết nối mạng.

#### 1.2.2. Quét cổng TCP/UDP của một địa chỉ IP

* Phát hiện dịch vụ: Giúp xác định các dịch vụ đang chạy trên một máy chủ, từ đó hỗ trợ việc quản lý và kiểm tra tính bảo mật của các dịch vụ này.
* Kiểm tra bảo mật: Phát hiện các cổng mở không cần thiết, từ đó giúp quản trị viên thực hiện các biện pháp bảo mật như đóng các cổng không dùng và cấu hình tường lửa.
* Đánh giá lỗ hổng: Giúp phát hiện các lỗ hổng bảo mật tiềm ẩn trong các dịch vụ đang chạy trên các cổng mở.

#### 1.2.3. Lắng nghe thông điệp từ một địa chỉ IP đến giao diện mạng

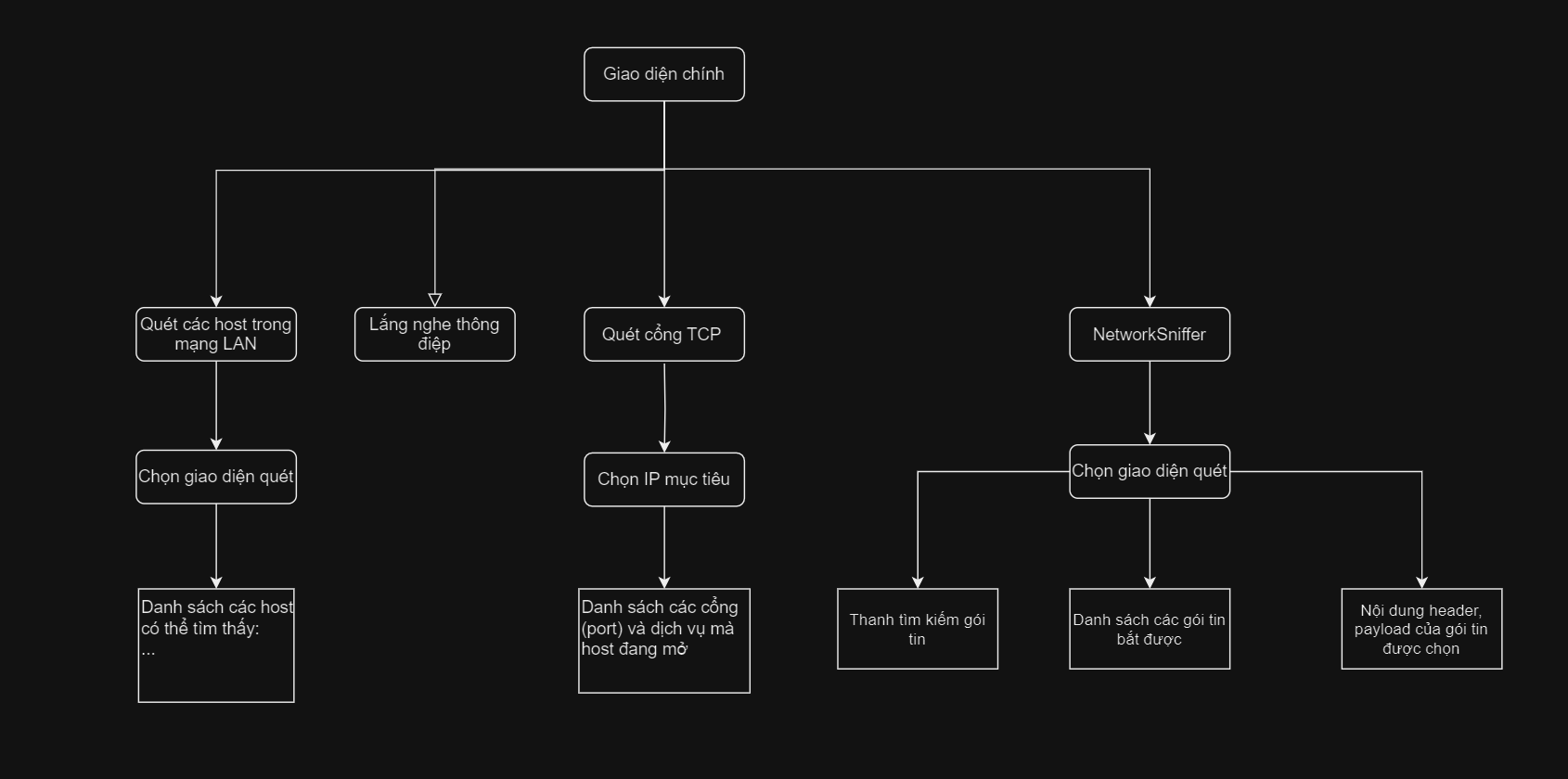
* Giám sát giao thông mạng: Giúp theo dõi lưu lượng mạng từ một địa chỉ IP cụ thể, giúp phát hiện các hoạt động bất thường hoặc tấn công.
* Phân tích hiệu suất: Cho phép phân tích chi tiết các gói tin để đánh giá hiệu suất mạng và tối ưu hóa lưu lượng.
* Phát hiện tấn công: Nhận diện các tấn công mạng như DDoS, phishing, hoặc xâm nhập trái phép.

#### 1.2.4. Bắt và hiển thị thông tin trên một giao diện mạng

* Phân tích gói tin: Cho phép bắt và phân tích các gói tin truyền qua giao diện mạng, giúp phát hiện các vấn đề về lưu lượng và bảo mật.
* Theo dõi lưu lượng: Hiển thị chi tiết các gói tin giúp quản trị viên theo dõi và hiểu rõ hơn về lưu lượng mạng, từ đó có thể tối ưu hóa hiệu suất.
* Tạo báo cáo: Cung cấp các báo cáo chi tiết về hoạt động mạng, hỗ trợ việc ra quyết định và lập kế hoạch bảo mật.

### 1.3. Thiết kế chương trình

#### 1.3.1. Mô hình phân rã chức năng



Hình 1 Mô hình phân rã chức năng

#### 1.3.2. Sequence Diagram

A diagram of a workflow

Description automatically generated with medium confidence

Hình 2 Sequence diagram của chương trình

#### Giải thích từng phần:

* **Quét các host trong mạng cục bộ**:
  + Người dùng bắt đầu quá trình quét bằng cách chọn một giao diện mạng.
  + Ứng dụng tính toán dải địa chỉ IP dựa trên IP và subnet mask của giao diện đó.
  + **Dịch vụ Ping** gửi các yêu cầu ICMP đến tất cả các IP trong dải và trả về kết quả cho các host hoạt động.
* **Quét cổng trên một host nhất định**:
  + Người dùng yêu cầu quét cổng trên một host.
  + **Bộ điều khiển chính** lặp qua các cổng và gửi gói TCP/UDP.
  + Kết quả được trả về cho các cổng mở/đóng và hiển thị trong giao diện.
* **Bắt gói tin trên giao diện đã chọn**:
  + Người dùng bắt đầu quá trình bắt gói tin.
  + **Dịch vụ bắt gói tin** thiết lập một socket thô trên giao diện mạng đã chọn và bắt đầu lắng nghe các gói tin.
  + Gói tin được xử lý và hiển thị thông tin chi tiết như địa chỉ nguồn, địa chỉ đích và giao thức.

#### 1.3.3. Cơ chế hoạt động của chương trình

A screenshot of a computer

Description automatically generated

Hình 3 Giao diện chính của chương trình

A screenshot of a computer

Description automatically generated

Hình 4 – Giao diện của Network Sniffer

**Khởi động ứng dụng**: Ứng dụng được khởi động và giao diện NetworkScantool được hiển thị.

**Lấy danh sách các giao diện mạng khả dụng**: Ứng dụng lấy danh sách tất cả các giao diện mạng đang hoạt động. Sử dụng lớp NetworkInterface để lấy danh sách các giao diện mạng. Danh sách các giao diện mạng sẽ được hiển thị.

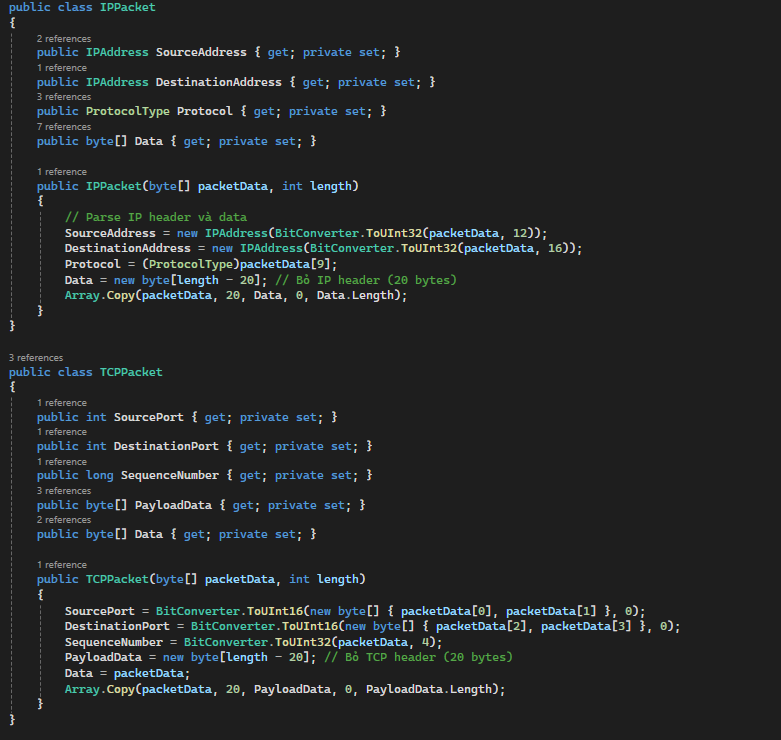
**Quét gói tin của giao diện mạng đã chọn**: Người dùng chọn một giao diện mạng từ danh sách rồi thực hiện quét gói tin. Thông tin IP của giao diện mạng được hiển thị.

**Thực hiện những tính năng**: Người dùng chọn 1 địa chỉ IP từ giao diện mạng để thực hiện các chức năng sẵn có như quét cổng TCP, lắng nghe thông điệp, mở NetworkSniffer để bắt gói tin từ máy,... (Nếu như có lỗi sẽ hiển thị thông báo lỗi).

## 2. PHÂN TÍCH CÁC CODE QUAN TRỌNG

### 2.1. Khám phá các thiết bị có trong mạng cục bộ

- Các class Packet cần thiết và hàm LoadNetworkInterfaces()



A computer screen shot of a program

Description automatically generated

Hình 5 – Các class cần thiết

* Các hàm và class phục vụ việc tính toán IP và bắt các gói tin để biết các cổng, dịch vụ đang mở của host.
* Hàm **GetIpRange** sẽ có 4 vòng lặp tương ứng với 4 lớp mạng đã được tách ra. Trong những vòng lặp đó, những lớp mạng đã được tách và xử lý từng lớp, tương ứng, địa chỉ mạng sẽ dùng phép AND (&) còn địa chỉ broadcast sẽ dùng phép OR ( | ) và các địa chỉ khả dụng cho thiết bị là các địa chỉ nằm giữa hai giá trị này.
* Đầu tiên, chương trình sẽ gọi hàm **loadNetworkInterfaces**() để load các giao diện có trên máy, sau đó, người dùng sẽ phải chọn giao diện mạng muốn quét (NetworkInterface), từ đó, chương trình sẽ lấy IP và subnetMask từ máy để tính toán được broadcast address (sử dụng hàm trên) và hiển thị tất cả vào giao diện người dùng.

A screen shot of a computer program

Description automatically generated

Hình 7 LoadNetworkInterFaces

* Chương trình phân chia dải IP cần quét thành 4 phần và sử dụng các tác vụ **bất đồng bộ** để xử lý từng phần song song. Mỗi tác vụ thực hiện việc ping từng địa chỉ IP trong dải của nó, kiểm tra trạng thái phản hồi, và cập nhật giao diện người dùng về tiến trình quét. Việc chia nhỏ công việc và chạy song song giúp tăng tốc độ quét so với việc thực hiện tuần tự, chương trình sẽ đợi tất cả các Task được tạo ra hoàn tất.

A computer screen shot of a program code

Description automatically generated

Hình 9 – List<Task> được phân chia mỗi task thực hiện việc Ping đến các host trong IpRange của mình

Nếu nhận được tín hiệu trả lời, chương trình sẽ thêm địa chỉ IP vào listView, cập nhật progressbar trong thời gian thực bằng hàm Invoke.

### 2.2. Quét cổng

A screen shot of a computer program

Description automatically generated

Hình 10 Các class, danh sách các port và dịch vụ tương ứng phổ biến

* Đoạn code này thực hiện quá trình quét cổng một cách hiệu quả bằng cách kiểm tra kết nối đến từng cổng trong danh sách các cổng phổ biến ở trên. Nếu một cổng phản hồi, nó được coi là đang mở, và thông tin được hiển thị trên giao diện người dùng trên thread chính. Quá trình này cũng hỗ trợ khả năng hủy bỏ bởi người dùng nếu cần thông qua CancellationToken

A screen shot of a computer program

Description automatically generated

Hình 11 Hàm quét các port TCP/UDP

### 2.3. Lắng nghe thông điệp từ địa chỉ đối tượng (Listen Message)

A computer screen shot of many colorful text

Description automatically generated

Hình 12 Hàm lắng nghe thông điệp

* Khi hàm này được gọi, đầu tiên chương trình sẽ hiển thị ra màn hình giao diện chọn giao diện mạng mà bạn muốn dùng để lắng nghe.
* Sau khi đã chọn giao diện mạng, chương trình sẽ sử dụng lớp Socket và cấu hình các thông số cần thiết để có thể thu nhận tất cả các gọi tin được chuyển tới giao diện mạng đã chọn. Kích hoạt chế độ lắng nghe toàn bộ (IOControlCode. ReceiveAll).
* Sau đó, khởi chạy một task để lắng nghe gói tin trong vòng lặp. Nếu nhận được gói tin, nó sẽ chuyển gói tin thành một đối tượng IPPacket và kiểm tra địa chỉ nguồn. Nếu địa chỉ nguồn trùng khớp với target, thông tin gói tin sẽ được ghi nhận và hiển thị thông tin chi tiết dưới dạng hex.
* Khi không có tín hiệu dừng, chương trình sẽ liên tục lắng nghe và kiểm tra số byte nhận được. Nếu số byte nhận được lớn hơn 0 đồng nghĩa với việc đã nhận được dữ liệu, chương trình sẽ tiến hành giải mã gói tin (de-encapsulation) thông qua lớp IPPacket, TCPPacket và UDPPacket.

### 2.4. Bắt gói tin

Sau khi nhấn nút NetworkSniffer, người dùng sẽ được chuyển tới giao diện khác. Sau khi chọn giao diện để bắt gói tin (tương tự như quét mạng – sử dụng NetworkInterfaces), người dùng nhấn nút Bắt đầu để gọi hàm sau:

A screen shot of a computer program

Description automatically generated

Hình 13 NetworkSniffer

Hàm này sẽ tạo 1 Task CapturePackets mới để thực hiện việc bắt gói tin, cụ thể:

A screen shot of a computer program

Description automatically generated

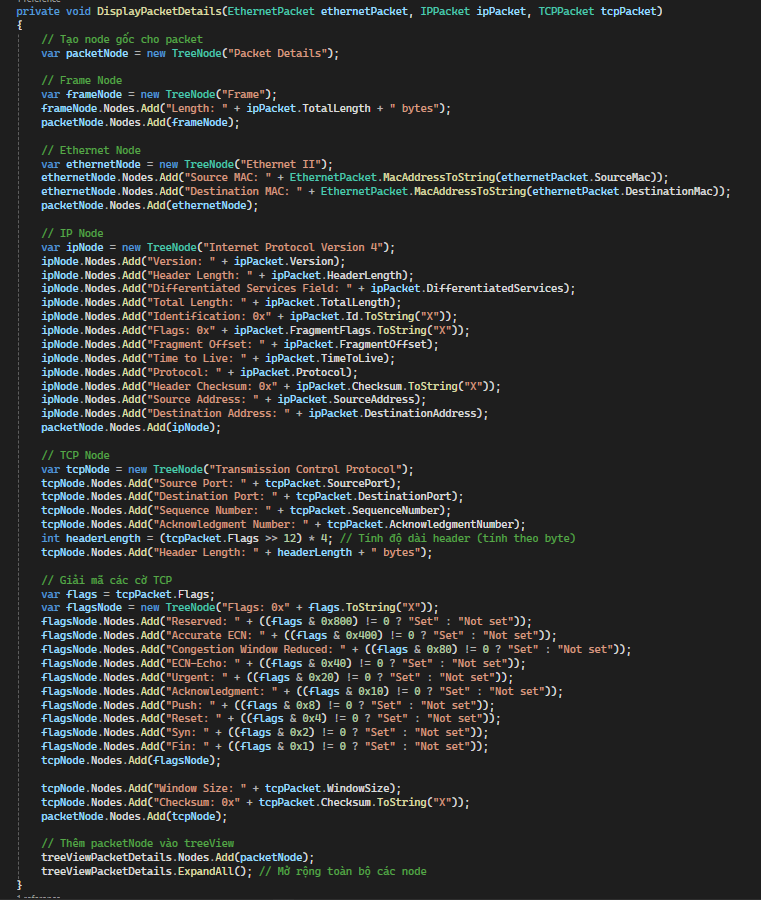
Hình 14 Task CapturePackets sẽ được gọi để bắt các gói tin trên giao diện được chọn

* Task này sẽ :
  + Tạo một Socket kiểu Raw để lắng nghe gói tin ở mức IP.
  + Gắn kết socket vào địa chỉ IP cụ thể và thiết lập để bao gồm phần tiêu đề (HeaderIncluded).
  + Kích hoạt chế độ nhận tất cả gói tin (IOControlCode.ReceiveAll).
  + Sẽ lắng nghe liên tục cho tới khi người dùng yêu cầu dừng thông qua cancellationToken
* Sau đó, tùy theo loại gói tin bắt được mà chia ra xử lý, ở đây là TCP và UDP packets.
* Những gói tin thu thập được sẽ được hiển thị lên control ListView. Khi người dùng nhấp vào một trong những gói tin đó, chương trình sẽ hiển thị chi tiết các thuộc tính trong trường header và payload của gói tin.

A screenshot of a computer

Description automatically generated

* Chương trình có tính năng lọc gói tin theo loại gói tin mà người dùng mong muốn (người dùng nhập loại gói tin vào thanh tìm kiếm)
* Hàm hiển thị thông tin gói tin được chọn:



Hình 18 Hàm hiển thị nội dung gói tin

# C. Một số thay đổi

1. Loại bỏ phần Invoke để cập nhật trên thread chính
2. Loại bỏ phần Wait(500) mỗi lần quét cổng phải đợi 500 ms

# D. VIDEO DEMO

**Link drive video demo:**

<https://drive.google.com/file/d/1KUWdRZojdVHdGUYiuS1jg_2gPXPO_R14/view?usp=sharing>

TÀI LIỆU THAM KHẢO

1.<https://drive.google.com/file/d/12EtYvyLuMdNczB_lUdo_yY04_QbPwd0R/view?usp=sharing>

2. [Network Sniffer and Analyzer Program - Part 3- CodeProject](https://www.codeproject.com/Articles/5350361/Network-Sniffer-and-Analyzer-Program-Part-3)

3. <https://github.com/zacharyreese/NetworkScanner?fbclid=IwAR2WlCO-9wRjSW2J6jb8eSlg-q6Xt7MxJ0Cl3uyksK1GoBP35Rs4crwiSpA>

4. Các slide bài giảng môn Lập trình mạng căn bản của thầy Đặng Lê Bảo Chương

**-------------HẾT-------------**